28.11. 2002 р. № 330-IV. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/330-15#Text (дата звернення: 28.02.2024).

7. Статут Товариства Червоного Хреста України : рішення XXII З'їзду Товариства Червоного Хреста України від 9 липня 2021 р., протокол № 1. URL: https://redcross.org.ua/wp-content/uploads/2016/10/Statute_URCS.pdf (дата звернення 03.01.2024).

8. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 р., що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 р. URL: https://zakon.rada.gov.ua/laws/show/995_199#Text (дата звернення: 28.02.2024).

9. Statutes of the International Red Cross and Red Crescent Movement URL: https://www.icrc.org/en/doc/assets/files/other/statutes-en-a5.pdf (дата звернення 03.01.2024).

10. Movement Coordination for Collective Impact Agreement Seville Agreement 2.0. URL: https://www.ifrc.org/document/seville-agreement-2 (дата звернення: 28.02.2024).

Пасічник Наталія Сергіївна
Кандидат історичних наук, доцент
кафедри філософських та політичних наук.
Білоцерківський національний аграрний університет
ORCID: 0009-0007-1694-9906

ІНФОРМАЦІЙНА ВІЙНА ТА ІНФОРМАЦІЙНІ ОПЕРАЦІЇ: АМЕРИКАНСЬКИЙ ПІДХІД

Повномасштабна російсько-українська війна та її вплив на геополітичну ситуацію у світовому масштабі наочно засвідчили зростаючу роль інформаційної складової сучасних воєн. Наразі провідні держави світу, в тому числі й США, приділяють першочергову увагу модернізації та розробці нових стратегій, технологій та інструментів інформаційно-психологічного впливу та інформаційної безпеки. Критичний аналіз теорії та практики інформаційних операцій США, одного зі світових лідерів у сфері ІКТ та одного з найважливіших стратегічних партнерів України, має практичне значення для нашої держави в умовах гібридної війни та становить дослідницький інтерес.

В США відсутнє офіційне визначення терміну «інформаційна війна» на урядовому рівні, але зазвичай під ним розуміють «використання та управління інформацією для досягнення конкурентної переваги, включаючи наступальні та оборонні зусилля» [2, с. 1]. В аналітичній доповіді Дослідницької служби

Конгресу США від 5 березня 2018 р. відзначається, що інформаційна війна (ІВ) відбувається на рівні, нижчому за рівень збройного конфлікту, і є комплексом військових і урядових операцій, спрямованих на захист і використання інформаційного середовища. Як форма політичної війни, ІВ є засобом, за допомогою якого держави досягають стратегічних завдань і просувають зовнішньополітичні цілі. Оборонні зусилля включають інформаційне забезпечення/інформаційну безпеку, в той час як наступальні зусилля включають інформаційні операції [2, с. 1].

Разом з тим, для опису схожих видів діяльності та активності в США використовуються й інші терміни, такі як «активні заходи», «гібридна війна», «війна в сірій зоні», «нерегулярна війна», «нетрадиційна війна», «асиметрична війна», «м'яка сила», «публічна дипломатія».

Інформаційна війна відбувається на стратегічному рівні, тоді як інформаційні операції (ІО) передбачають використання різних можливостей, пов'язаних з інформацією, для реалізації стратегії. Операції пов'язують ці стратегічні цілі з конкретними тактичними прийомами, методами і процедурами для їх досягнення.

У Дорожній карті інформаційних операцій міністерства оборони США від 30.10.2003 р. складовими інформаційних операцій визначено п'ять компонентів: комп'ютерні мережеві операції, які складалися з комп'ютерної мережевої атаки, захисту комп'ютерних мереж, використання комп'ютерних мереж; психологічні операції; радіоелектронна боротьба; безпека операцій та військовий обман [2, с. 3]. Пізніше комп'ютерні мережеві операції стали операціями в кіберпросторі, наступальними і оборонними, з власною окремою доктриною, викладеною в Спільній публікації Об'єднаного комітету начальників штабів, де кібероперації окреслюються як використання можливостей кіберпростору для досягнення цілей в кіберпросторі або через нього [3]. Психологічні операції (ПО) передбачають цілеспрямоване використання інформації (пропаганди) для впливу на емоції, мотиви, аргументацію і, зрештою, на поведінку іноземних урядів, організацій, груп та окремих осіб. На стратегічному рівні ПО - це надання інформації для впливу на іноземні цільові аудиторії на підтримку цілей і завдань США. На оперативному рівні ПО проводяться на підтримку виконання бойових завдань, або як невід'ємна частина інших операцій. Радіоелектронна боротьба включає радіоелектронне придушення та радіоелектронний захист. Безпека операцій - процес ідентифікації критично важливої інформації та аналізу дій, що супроводжують військові операції та інші заходи. Військовий обман - дії, спрямовані на навмисне введення в оману військового керівництва супротивника, таким чином спонукаючи супротивника до конкретних дій (або бездіяльності), які сприятимуть досягненню визначеної мети. Цей компонент тісно пов'язаний з ПО, й зосереджується на неправдивій

інформації або дезінформації [2, с. 3-4].

У словнику військових термінів міністерства оборони США інформаційні операції визначаються як комплексне застосування під час військових операцій інформаційних можливостей у взаємодії з іншими видами операцій з метою впливу, дезорганізації, корумпування або узурпації процесу прийняття рішень супротивниками і потенційними супротивниками при одночасному захисті своїх власних [1, с. 104] Це визначення переносить наголос з набору тактичних прийомів або принципів на бажані ефекти і способи їх досягнення. Стратегічні комунікації, публічна дипломатія, зв'язки з громадськістю та операції в кіберпросторі розглядаються як допоміжні сили і засоби.

Сучасний підхід до інформаційних операцій основним їх компонентом розуміє інформаційне забезпечення військової діяльності, що є спланованими операціями з донесення потрібної інформації та даних до іноземних аудиторій. Операції з інформаційного забезпечення військової діяльності зосереджуються на когнітивному елементі інформаційного середовища, де його цільовою аудиторією є не лише потенційні та реальні супротивники, а й населення союзних та нейтральних держав.

В ІО можуть використовуватися різні категорії інформації:

- Пропаганда - поширення певних ідей або наративу з метою психологічного впливу. Пропагандою, а також публічною дипломатією вважається інформування урядом про свої наміри, політику та цінності через промови, прес-релізи та інші публічні заходи. Ці комунікації мають стратегічну цінність, оскільки з часом вони можуть спонукати осіб, які приймають рішення, до певного курсу дій.

- Поширення ненавмисно неправдивої інформації (наприклад, інтернет-тролі, які поширюють теорії змови або веб-містифікації через соціальні мережі).

- Дезінформація, яка є навмисно неправдивою. Прикладами можуть бути неправдиві новини в ЗМІ, фальсифікація протестів, підробка фотографій тощо.

Всі ці різновиди активності відбуваються в інформаційному середовищі, яке є сукупністю осіб, організацій та систем, що збирають, поширюють або діють на основі інформації. Сюди входять:

- Фізичний рівень: системи управління та контролю і пов'язана з ними інфраструктура.

- Інформаційний рівень: мережі та системи, де зберігається інформація.

- Когнітивний рівень: свідомість людей, які передають інформацію та реагують на неї.

Усі інструменти національної могутності - дипломатичні, інформаційні, військові та економічні - можуть бути використані в інформаційному середовищі [2, с. 5-6].

У листопаді 2023 р. Міністерство оборони США оприлюднило «Стратегію операцій в інформаційному середовищі», в якій підкреслюється, що інформація стає основоположним елементом усіх військових стратегій та операцій в інформаційному середовищі. Операції в інформаційному середовищі визначаються як військові дії, що передбачають інтегроване застосування складних інформаційних сил для впливу на фактори поведінки шляхом інформування аудиторії, впливу на іноземних релевантних суб'єктів; руйнування та використання інформації, інформаційних мереж та інформаційних систем відповідних суб'єктів; і захисту своєї інформації, інформаційних мереж та інформаційних систем [4].

Основна увага в Стратегії зосереджена на посиленні і збалансуванні інституційної і оперативної синергії між операціями з інформаційного забезпечення, цивільними справами, зв'язками з громадськістю, об’єднаними операціями в електромагнітному спектрі, операціями в кіберпросторі, космічними операціями, спеціальними технічними операціями, заходами з військової дезінформації, безпековими операціями, новітньою інформаційною діяльністю, іншими дисциплінами та інформаційними аспектами фізичної сили.

Очікується, що Стратегія покращить спроможність міністерства оборони США планувати, забезпечувати ресурсами та застосовувати інформаційну міць для побудови довготривалої переваги, а також стримувати виклики життєво важливим національним інтересам США на будь-якій арені чи в будь-якій сфері. Серед «загроз» національній безпеці Сполучених Штатів називаються Китайська Народна Республіка, Росія, Іран, Північна Корея і насильницькі екстремістські організації, причому КНР визначено як «найбільш комплексний і серйозний виклик національній безпеці», Росію – як «гостру загрозу», решта - залишаються «постійними загрозами» [4]. У документі підкреслюється, що вказані країни постійно посилюють і використовують свої дипломатичні, військові, технологічні та інформаційні можливості з метою підвищення ризиків для збройних сил США і їхніх союзників і послаблення стримування.

Згідно зі Стратегією, Міністерство оборони має розробити процес швидкого розгортання команд інформаційних сил, в тому числі резервних сил, а також створити відповідну робочу силу, що складається з військових і цивільних експертів. Вона визначає чотири напрямки діяльності, які дозволять Міністерству інтегрувати і модернізувати операції в інформаційному середовищі:

- Люди і організації;
- Програми;
- Політика і управління;
- Партнерство.

Міністерство оборони має інвестувати в дослідження, розробку,

обслуговування і підтримку інформаційних сил і засобів, забезпечувати їх безпеку і інтегрувати для успішного проведення операцій в інформаційному середовищі, досягнення і утримання інформаційної переваги. Йдеться про те, що керівники всіх підрозділів Міністерства оборони нарощуватимуть сили і можливості для протистояння інформаційній війні противника шляхом поліпшення здатності Міністерства інтегрувати, перевіряти, використовувати і оцінювати операції в інформаційному середовищі [4].

Таким чином, в США інформаційна війна розглядається насамперед як форма політичної війни та засіб досягнення зовнішньополітичних цілей держави, інформаційні операції - як інструмент інформаційної війни, які містять дії, спрямовані на досягнення інформаційної переваги чи перемоги над супротивником шляхом впливу на інформацію, інформаційні процеси та інформаційні системи супротивника, забезпечуючи при цьому безпеку власних аналогічних інформаційних ресурсів та систем. При цьому акцентується увага на когнітивному елементі інформаційного середовища як держав-супротивників, так і союзних та нейтральних країн. Оприлюднена в 2023 р. нова Стратегія операцій в інформаційному середовищі засвідчує усвідомлення військовим керівництвом США зростаючих загроз національній безпеці країни в інформаційній сфері з боку потенційних та реальних супротивників та комплексних підхід до планування інформаційних операцій. Перспективи подальших досліджень вбачаються в аналізі ефективності згаданої стратегії та практичного досвіду Вашингтону у царині інформаційних операцій загалом.

Список використаних джерел

1. DOD Dictionary of Military and Associated Terms / Federation of American Scientists. URL: https://irp.fas.org/doddir/dod/dictionary.pdf (Last accessed: 24.03.2024).
2. Information Warfare: Issues for Congress. By Catherine A. Theohary. March 5, 2018 / Congressional Research Service. URL: https://sgp.fas.org/crs/natsec/R45142.pdf (Last accessed: 23.03.2024).
3. Joint Chiefs of Staff, Joint Publication 3-12. Cyberspace Operations, 8 June 2018. / Federation of American Scientists. URL: https://irp.fas.org/doddir/dod/jp3_12.pdf (Last accessed: 23.03.2024).
4. Strategy for Operations in the Information Environment. July 2023 / U.S. Department of Defense. URL: https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-DEPARTMENT-OF-DEFENSE-STRATEGY-FOR-OPERATIONS-IN-THE-INFORMATION-ENVIRONMENT.PDF (Last accessed: 20.03.2024).